FILED
2024 Oct-03 AM 08:54
U.S. DISTRICT COURT
N.D. OF ALABAMA

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
WESTERN DIVISION

DOUGLAS GIBSON,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Civil Action No. 7:24-cv-95-ACA**
	)	
WARRIOR MET COAL INC,	)	
	)	
Defendant.	)	

MEMORANDUM OPINION

Defendant Warrior Met Coal Inc., collects and maintains personal identifying information about its employees. In a data breach, unauthorized third parties stole the personal identifying information of over 19,000 current and former employees. Plaintiff Douglas Gibson is one such former employee. He brings this action asserting state law claims against Warrior on behalf of himself and a putative class, seeking both injunctive relief and monetary damages for: (1) negligence ("Count One"); (2) negligence *per se* ("Count Two"); (3) breach of implied contract ("Count Three"); (4) invasion of privacy ("Count Four"); and (5) unjust enrichment ("Count Five"). (Doc. 1 at ¶¶ 163–250).

Warrior moves to dismiss the complaint. (Doc. 12). The court **WILL GRANT IN PART** and **DENY IN PART** Warrior's motion to dismiss. The court **WILL DISMISS WITHOUT PREJUDICE** for lack of standing all of

Mr. Gibson's requests for injunctive relief except the request to educate class members about the threats they face and steps they must take to protect themselves. The court **WILL DISMISS** Count Four for failure to state a claim. The court **WILL DENY** the motion to dismiss Counts One, Two, Three, and Five.

I. BACKGROUND

In deciding a motion to dismiss, the court must accept as true the factual allegations in the complaint and construe them in the light most favorable to the plaintiff. *Butler v. Sheriff of Palm Beach Cnty.*, 685 F.3d 1261, 1265 (11th Cir. 2012) (addressing a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6)); *Tsao v. Captiva MVP Rest. Partners*, 986 F.3d 1332, 1339 (11th Cir. 2021) (addressing a facial attack on subject matter jurisdiction). The court notes that Mr. Gibson prefaces some of his allegations "upon information and belief." (Doc. 1 at 1; *id.* ¶¶ 9, 47, 53, 93, 98, 142, 146, 150, 215–16). Warrior contends that the court can disregard these allegations. (Doc. 12-1 at 23–24).

But Federal Rule of Civil Procedure 11(b) specifically allows a party or attorney to plead facts on "knowledge, information and belief, formed after an inquiry reasonable under the circumstances." Fed. R. Civ. P. 11(b). Accordingly, where an allegation based upon "information and belief" would be sufficient absent the "information and belief" caveat, the allegation is entitled to the presumption of truth. *See, e.g.*, *Doe v. Samford Univ.*, 29 F.4th 675, 692 (11th Cir. 2022)

("Assuming—as [a federal court] must [on a motion to dismiss]—that [the plaintiff's] 'information and belief' allegation is truthful" where such allegation includes specific factual information); *cf. Mann v. Palmer*, 713 F.3d 1306, 1315 (11th Cir. 2013) (holding that the court need not accept as true allegations pleaded "upon information and belief" when the allegations lacked sufficient facts) (quotation marks omitted). The court's description of the facts therefore sets out all specifically alleged facts and reasonable inferences to be drawn from them.

The court may also consider documents "not referred to or attached to a complaint under the incorporation-by-reference doctrine if the document is (1) central to the plaintiff's claims; and (2) undisputed, meaning that its authenticity is not challenged." *Johnson v. City of Atlanta*, 107 F.4th 1292, 1300 (11th Cir. 2024) (footnote omitted). Warrior attaches to its motion to dismiss a sample letter it sent to people affected by the data breach. (Doc. 12-2). The letter is central to Mr. Gibson's claims and he does not challenge the authenticity of the letter or allege that the letter he received differed in any way from the sample letter. (*See* doc. 16). Accordingly, the court's description of the facts to be considered at the pleading stage includes Warrior's notification letter.

As a condition of employment, Warrior requires its employees to provide personal information, such as their names, dates of birth, and social security numbers. (*See* doc. 1 ¶ 140). Mr. Gibson worked for Warrior from 2013 until 2019

and provided his name, date of birth, and social security number because Warrior represented, and he believed, that Warrior would protect the information. (*Id.* ¶¶ 139–40; *see also id.* ¶¶ 18, 27–29, 54, 141). But Warrior did not encrypt the information and it failed to implement cyberattack prevention and detection measures recommended by the government and the Microsoft Threat Protection Intelligence Team. (*Id.* ¶¶ 41, 43–46).

In July 2023, a third party accessed Warrior's network and took files containing current and former employees' personal identifying information, including health information. (*Id.* ¶¶ 35, 39; *see also id.* ¶¶ 5, 164). Warrior notified Mr. Gibson the data breach (doc. 1 ¶ 35), stated that it had "recovered the files" and was "not aware of any actual or attempted misuse of personal information" (*id.*; doc. 12-2 at 2), and offered twelve months of identity monitoring services (*id.* ¶ 63; *see* doc. 12-2 at 3). The letter also encouraged recipients to review their credit reports, place fraud alerts and security freezes, and monitor account statements. (Doc. 1 ¶ 144; doc. 12-2 at 4). Mr. Gibson tried to mitigate the impact of the data breach by researching information about the breach, contacting credit bureaus about his accounts, and monitoring his financial accounts for fraudulent activity (Doc. 1 ¶ 144). He also experienced an increase in spam calls, texts, and emails. (*Id.* ¶ 146). The breach, and the increased risk of identity theft he now faces, has caused him fear, anxiety, and stress. (*Id.* ¶ 147).

Mr. Gibson asserts claims of negligence, negligence *per se*, breach of implied contract, invasion of privacy, and unjust enrichment. (*Id.* at 38–52). He seeks both injunctive and monetary relief. (*Id.* at 52–56).

II. DISCUSSION

Warrior moves to dismiss Mr. Gibson's complaint on two grounds: first, that Mr. Gibson lacks Article III standing to sue (*see* doc. 12-1 at 12–29), and second, that Mr. Gibson has failed to state a claim upon which relief can be granted (*see id.* at 30–43). Before addressing Warrior's substantive arguments, the court notes that Warrior characterizes the cyberattack as "a ransomware attack" and alleges that (1) it "recovered the affected files and obtained proof of deletion," which it has confirmed again since the cyberattack, and (2) no personal information accessed during the cyberattack has been misused. (Doc. 12-1 at 9, 11–12). The court cannot consider those allegations because they are not contained with the complaint and documents that are incorporated in the complaint by reference. *See* Fed. R. Civ. P. 12(d); *see also Morrison v. Amway Corp.*, 323 F.3d 920, 924 n.5 (11th Cir. 2003) ("Facial attacks challenge subject matter jurisdiction based on the allegations in the complaint . . . .").

So, bearing in mind the court's obligation to consider only the pleadings and evidence properly incorporated by reference, the court turns to whether it has subject matter jurisdiction over this case. After finding that the court does have jurisdiction

over one of the requests for injunctive relief and all requests for monetary damages, the court addresses Warrior's arguments about the merits.

1. Standing

Warrior contends that Mr. Gibson lacks standing because he alleges only the possibility that he may suffer an injury in the future and any injury he suffered or might suffer in the future is not traceable to Warrior. (Doc. 21-1 at 14–27).

Article III of the Constitution limits federal courts to deciding "Cases" or "Controversies." U.S. Const. art. III, § 2. Absent a case or controversy, the court lacks subject matter jurisdiction over a case. *Hunstein v. Preferred Collection & Mgmt. Servs., Inc.*, 48 F.4th 1236, 1242 (11th Cir. 2022) (en banc). One element of a case or controversy is standing. *Id.* To show standing, the plaintiff must allege facts allege facts that plausibly establish that 1) he "experienced an injury that is concrete and particularized and actual or imminent, 2) the defendant's conduct is the cause of the plaintiff's injury, and 3) a decision by the court would likely redress the plaintiff's injury." *Green-Cooper v. Brinker Int'l, Inc.,* 73 F.4th 883, 889 (11th Cir. 2023), *cert. denied sub nom. Brinker Int'l, Inc. v. Steinmetz*, 144 S. Ct. 1457 (2024); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) (holding that because standing is "an indispensable part of the plaintiff's case, each element must be supported . . . with the manner and degree of evidence required at the successive stages of the litigation"); *Trichell v. Midland Credit Mgmt., Inc.*, 964 F.3d 990, 996

(11th Cir. 2020) ("[A]t the motion-to-dismiss stage, [the plaintiffs] bore the burden of alleging facts that plausibly establish their standing.").

Standing must exist "for each claim" and "for each form of relief." *Davis v. FCC*, 554 U.S. 724, 734 (2008). The court begins by addressing whether Mr. Gibson has standing to request injunctive relief, followed by his standing to request monetary damages.

a. Injunctive Relief

Mr. Gibson seeks an injunction (1) enjoining Warrior from "engaging in the wrongful conduct" described in the complaint relating to "misuse and/or disclosure of" personal identifying information and (2) requiring it to take various actions to prevent any further data breaches. (Doc. 1 at 52–55).

A plaintiff lacks standing to request injunctive relief unless the threat of future harm is "substantial" or "certainly impending." *Tsao*, 986 F.3d at 1339 (quotation marks omitted); *see also TransUnion LLC v. Ramirez*, 594 U.S. 413, 435 ("[A] person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial."). A data breach alone is not enough to satisfy that standard. *Tsao*, 986 F.3d at 1344. But an allegation of "actual misuse or actual access to personal data" can suffice. *Id.* at 1340, 1344 (quotation marks omitted); *accord Brinker*, 73 F.4th at 889.

Here, Mr. Gibson alleges actual access to his name, date of birth, social security number, and medical information. (Doc. 1 ¶¶ 4, 29, 140). He also alleges facts (the increase in spam calls beginning after the data breach) from which it is reasonable to infer that actual misuse occurred. (*Id.* ¶ 146). He has therefore pleaded a "substantial risk" of future harm, establishing an injury in fact for purposes of his request for injunctive relief. *See Tsao*, 986 F.3d at 1339, 1344 (quotation marks omitted).

The traceability requirement is satisfied if the plaintiff demonstrates "factual causation between his injuries and the defendant's misconduct." *Walters*, 60 F.4th at 650. This is a "less stringent" standard "than the tort-law concept of proximate cause." *Id.* (quotation marks omitted). "Even harms that flow indirectly from the action in question can be fairly traceable to that action for standing purposes." *Id.* (quotation marks omitted; alterations accepted). Mr. Gibson satisfies that standard. He alleges that Warrior's failure to adequately protect personal identifying information led to hackers stealing the data, leading to past misuse and the continuing risk of misuse of the data. (*See* doc. 1 ¶¶ 4, 29, 140, 146). Although Warrior itself has not misused and is not going to misuse the data, the injury in fact is fairly traceable to it. *See Walters*, 60 F.4th at 650.

But Mr. Gibson has not adequately alleged redressability for most of his requests for injunctive relief. To do that, the plaintiff must allege facts showing "that

his injuries are likely to be redressed by a favorable judicial decision." *Walters v. Fast AC, LLC*, 60 F.4th 642, 649 (11th Cir. 2023) (quotation marks omitted). Mr. Gibson's injury is the likelihood that the hacker or others who access the data on the dark web will use that data. But most of the injunctive relief Mr. Gibson requests aims to prevent another data breach, not to prevent the misuse of the stolen data. (*See* doc. 1 at 52–55). Preventing another data breach will not remove the personal identifying information from the dark web or from the possession of the hacker who stole it or anyone who has already purchased it. Accordingly, the relief requested would not redress the injury and Mr. Gibson lacks standing to seek those forms of injunctive relief. *See Walters*, 60 F.4th at 649.

One of Mr. Gibson's requests for injunctive relief is to "requir[e Warrior] to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect himself." (Doc. 1 at 55). Granting this relief would redress the harm Mr. Gibson alleges by helping him to protect himself from further misuse of his data. Accordingly, he has standing to pursue that request for injunctive relief. The court **WILL DISMISS** all of Mr. Gibson's requests for injunctive relief except the request to educate class members about the threats they face and steps they must take to protect themselves.

b. Monetary Relief

Mr. Gibson also requests damages. (Doc. 1 ¶¶ 196, 223, 233, 250; *id.* at 55–56). Warrior argues that he lacks standing to seek damages because he has not alleged that he suffered an injury in the past; he has alleged only a potential future injury that is not traceable to Warrior. (Doc. 12-1 at 16–25).

When seeking monetary damages, two kinds of harm exist: "1) tangible harms, like physical or monetary harms; [and] 2) intangible harms, like injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *Green-Cooper*, 73 F.4th at 889. In addition, the risk of future harm can be an injury in fact if "the exposure to the risk of future harm itself causes a *separate* concrete harm." *TransUnion*, 594 U.S. at 436. Mr. Gibson alleges that he spent time researching information about the breach, contacting credit bureaus about his accounts, and monitoring his financial accounts for fraudulent activity. (Doc. 1 ¶ 144). He also alleged facts indicating that he needed to spend that time because his evidence has already been misused, as shown by a post-data breach increase in spam calls, texts, and emails. (*See id.* ¶ 146). These allegations are sufficient, at the pleading stage, to demonstrate that Mr. Gibson spent time attempting to mitigate a real risk that he faced. *See Salcedo v. Hanna*, 936 F.3d 1162, 1173 (11th Cir. 2019) ("We have found standing where the harm was, for example, time wasted traveling to the county registrar's office, and correcting credit reporting

errors.") (citation omitted). In addition to the time Mr. Gibson has spent, he alleges that he has experienced fear, anxiety, and stress because of the breach and the increased risk of identity theft he now faces. (Doc. 1 ¶ 147). Emotional distress is an injury in fact for standing purposes. *See Walters*, 60 F.4th at 648 (holding that, at the summary judgment stage, deposition testimony describing "emotional distress is sufficient evidence of [that injury]" to establish standing); *Lujan*, 504 U.S. at 561 ("[E]ach element [of standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation.").

Mr. Gibson has also adequately pleaded traceability. He alleges facts supporting a reasonable inference that Warrior's failure to take reasonable precautions to protect the confidential data it held led to the data breach and ultimately the misuse of data. (Doc. 1 ¶¶ 35, 39, 41, 43–46). That is sufficient for traceability purposes. *See Wilding v. DNC Servs. Corp.*, 941 F.3d 1116, 1125 (11th Cir. 2019) (quotation marks omitted).

Finally, Mr. Gibson has adequately pleaded redressability because an award of damages would redress his time spent and emotional distress. *See Walters*, 60 F.4th at 650 ("[A]n injury in fact in the form of wasted time, economic harm, and emotional distress . . . [,] it goes without saying, is an injury which the award of damages will redress.") (quotation marks omitted; one alteration accepted); *see also*

In re Equifax Inc. Customer Data Sec. Breach Litig., 999 F.3d 1247, 1262 (11th Cir. 2021) ("[W]hen a plaintiff faces a sufficient risk of harm, the time, money, and effort spent mitigating that risk are also concrete injuries."). Because Mr. Gibson has standing to seek monetary damages, the court **WILL DENY** the motion to dismiss his requests for monetary damages.

2. Merits

Mr. Gibson asserts five state law claims under Alabama law: (1) negligence, (2) negligence *per se*, (3) breach of implied contract, (4) invasion of privacy, and (5) unjust enrichment. (Doc. 1 ¶¶ 163–250); *see Flintkote Co. v. Dravo Corp.*, 678 F.2d 942, 945 (11th Cir. 1982) ("Where federal jurisdiction is based on diversity of citizenship, the substantive law of the forum state applies."). Warrior moves to dismiss all five claims on the ground that Mr. Gibson has failed to state a claim. (Doc. 12-1 at 30–43). The court will address each argument in turn.

a. Count One: Negligence

Mr. Gibson alleges that Warrior was negligent because it failed to use reasonable security measures to protect the personal identifying information, which it required its employees to submit as a condition of employment, and its lack of reasonable security measures resulted in the cyberattack compromising the data. (Doc. 1 ¶¶ 163–98). To adequately plead a negligence claim under Alabama law, Mr. Gibson must allege "that the defendant owed the plaintiff a legal duty, that the

defendant breached that duty, that the plaintiff suffered a loss or injury, that the defendant's breach was an actual cause of the injury, and that the defendant's breach was a proximate cause of the injury." *Haddan v. Norfolk S. Ry. Co.*, 367 So. 3d 1067, 1072 (Ala. 2022). Warrior challenges only the existence of an injury and causation, arguing that Mr. Gibson failed to allege (1) that he suffered an injury because he did not allege that his data was misused and (2) proximate causation because the intervening criminal action of the hacker broke the chain of causation. (Doc. 12-1 at 30–35).

Mr. Gibson adequately alleged facts supporting a reasonable inference that his data has been misused: after the data breach, he experienced an increase in spam calls, texts, and emails. (*See* doc. 1 ¶ 146); *Gates v. Khokhar*, 884 F.3d 1290, 1296 (11th Cir. 2018) ("When ruling on a motion to dismiss, [the court] accept[s] the facts alleged in the complaint as true, drawing all reasonable inferences in the plaintiff's favor.") (quotation marks omitted).

Mr. Gibson also adequately alleged facts that, if true, would establish proximate causation. As a general rule, Alabama law prohibits holding a person liable for the criminal acts of another. *Carroll v. Shoney's, Inc.*, 775 So. 2d 753, 756 (Ala. 2000). But a defendant can be held liable for another's criminal act where the "particular criminal conduct" was foreseeable, the defendant "possessed specialized knowledge of the criminal activity," and the criminal conduct was "a probability."

Id. (quotation marks omitted). Mr. Gibson alleges that Warrior required its employees to disclose personal identifying information, promised to protect that information, and knew that hackers value unprotected data, but failed to implement industry standards to protect that information despite warnings from multiple agencies that entities storing personal data are attractive to hackers. (Doc. 1 ¶¶ 57, 60, 164, 177–78). At the dismissal stage, those allegations are sufficient to survive a motion to dismiss for failure to state a claim. Accordingly, the court **WILL DENY** Warrior's motion to dismiss Count One.

b. Count Two: Negligence Per Se

Mr. Gibson alleges that Warrior is liable for negligence *per se* under Alabama law because the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, created a duty to safeguard the personal identifying information Warrior's employees gave it. (Doc. 1 ¶¶ 199–206). A claim of negligence *per se* under Alabama law requires that (1) the defendant violated a statute; (2) the statute "was enacted to protect a class of persons to which the plaintiff belonged"; (3) "the plaintiff's injury was the kind of injury contemplated by the statute"; and (4) "the defendant's violation of the statute proximately caused the plaintiff's injury." *Dickinson v. Land Devs. Constr. Co., Inc.*, 882 So. 2d 291, 302 (Ala. 2003). Alabama law allows a negligence *per se* claim to be based on a statute that does not

provide a private right of action. *Allen v. Delchamps, Inc.*, 624 So. 2d 1065, 1068 (Ala. 1993); (*see* doc. 12-1 at 36 n.15).

Warrior argues that Mr. Gibson failed to adequately allege (1) an actual injury based on misuse of his data, (2) that the FTC Act protects a class of persons instead of the public at large, or (3) that Warrior violated the FTC Act. (Doc. 12-1 at 36–37). The court already rejected Warrior's argument about Mr. Gibson's injury and will not address that argument again.

So the court turns to Warrior's argument about whether the FTC Act protects a class of persons instead of the public at large. (Doc. 12-1 at 37). "The doctrine of negligence per se or negligence as a matter of law arises from the premise that the legislature may enact a statute that replaces the common-law standard of the reasonably prudent person with an absolute, required standard of care." *Parker Bldg. Servs. Co. v. Lightsey ex rel. Lightsey*, 925 So. 2d 927, 930–31 (Ala. 2005). But "not every violation of a statute . . . is negligence per se." *Id.* at 931. "The statute must have been enacted to protect a class of persons, of which the plaintiff is a member." *Id.* A statute that protects "the general public" does not protect a class of persons. *Id.*

Warrior argues that the FTC Act was enacted to protect the general public. (Doc. 12-1 at 36–37). The FTC Act prohibits "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). The Eleventh Circuit has explained that the FTC

Act protects consumers and competitors. *LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221, 1228 (11th Cir. 2018) ("[T]he FTC possesses 'unfairness authority' to prohibit and prosecute unfair acts or practices harmful to consumers" and competitors). Most of the Eleventh Circuit's discussion of the purpose of the FTC Act has come in the context of claims brought under the Fair Debt Collection Practices Act ("FDCPA"), 15 U.S.C. § 1692 *et seq. See LeBlanc v. Unifund CCR Partners*, 601 F.3d 1185, 1194 (11th Cir. 2010); *Jeter v. Credit Bureau, Inc.*, 760 F.2d 1168, 1172 (11th Cir. 1985).

Because the FDCPA was enacted to "supplement" the FTC Act's protection of "unsophisticated consumers from debt collection practices which have a tendency or capacity to deceive," the Eleventh Circuit uses the same standards to evaluate whether a practice is deceptive under the FTC Act and the FDCPA. *Jeter*, 760 F.2d at 1173–75; *see LeBlanc*, 601 F.3d at 1194. In this context, the Eleventh Circuit has explained that neither the FTC Act nor the FDCPA uses a "reasonable consumer" standard to evaluate whether a practice is deceptive; the appropriate standard is whether a practice might deceive the "least-sophisticated consumer." *LeBlanc*, 601 F.3d at 1194; *see Jeter*, 760 F.2d at 1175. To reach that conclusion, the Eleventh Circuit has explained that the FTC Act "was not made for the protection of experts, but for the public—that vast multitude which includes the ignorant, the unthinking, and the credulous." *Jeter*, 60 F.2d at 1172–73 (quotation marks omitted). Warrior

relies on this language to argue that the FTC Act seeks to protect the public instead of a particular class of persons. (Doc. 12-1 at 36–37).

The court disagrees that this language indicates that the FTC Act protects the general public instead of a class of persons. The language about the statute protecting the public, as opposed to experts, relates to what standard courts should use in evaluating deceptiveness, not the class of persons protected by the statute. *See LeBlanc*, 601 F.3d at 1194; *Jeter*, 60 F.2d at 1172–73. The Eleventh Circuit has never held that the FTC Act protects the general public; instead, it has held that the FTC Act protects consumers and competitors. *LabMD, Inc.*, 894 F.3d at 1228. Those are two classes of persons distinct from the general public; if a person is not a consumer or a competitor, the FTC Act's protections do not reach that person. *See id.*; *see also Fed. Trade Comm'n v. On Point Cap. Partners LLC*, 17 F.4th 1066, 1079 (11th Cir. 2021).

The Alabama Supreme Court has drawn similar distinctions. In *Lightsey*, the Court distinguished between building codes meant to protect "the general welfare" and "rules of the road," which "were passed for the benefit of a particular class of people who use the public streets and highways for travel." 925 So. 2d at 932 (quotation marks omitted). Similarly, in *Allen v. Delchamps, Inc.*, 624 So. 2d 1065, 1066–67 (Ala. 1993), the plaintiff purchased and consumed celery hearts that had been treated with sodium bisulfite, in violation of the federal Food, Drug, and

Cosmetic Act and regulations promulgated under that act. The Alabama Supreme Court held that because the sodium bisulfite ban was meant to protect "sulfite-sensitive individuals," the sulfite regulations protected a particular class of persons for purposes of a negligence *per se* claim. *Id.* at 1067. Applying the Alabama Supreme Court's analysis to this case, it appears that the FTC Act's protection of consumers and competitors is more limited than protection of the general public.

The court rejects Warrior's argument that the FTC Act protects the public at large. Because Warrior has not made an argument about whether Mr. Gibson is a member of the class that the FTC Act protects (*see* doc. 12-1 at 36–37), the court proceeds to Warrior's final argument: that Mr. Gibson failed to state a claim that Warrior violated the FTC Act at all (*id.* at 37). Warrior abandoned this argument by providing nothing more than a conclusory statement that Mr. Gibson's claim fails. (*See* doc. 12-1 at 37). The court cannot evaluate whether Mr. Gibson's allegations are deficient without legal citations, an explanation of what elements are required to make out an FTC Act violation, and an argument about how Mr. Gibson's allegations fall short of the standard. *See Sapuppo v. Allstate Floridian Ins. Co.*, 739 F.3d 678, 682 (11th Cir. 2014) (holding that "[a]bandonment of an issue can . . . occur when passing references appear in the argument section," particularly when "the passing references are nothing more than conclusory assertions"). The court **WILL DENY** Warrior's motion to dismiss Count Two. (Doc. 12-1).

c. Count Three: Implied Contract

Mr. Gibson alleges that Warrior breached implied contracts to protect his personal identifying information and medical data and to timely and accurately notify him if the data was breached and compromised or stolen. (Doc. 1 ¶ 209). To establish a breach of contract, the plaintiff must allege facts that, if true, would prove the existence of the contract, the plaintiff's performance, the defendant's nonperformance, and damages. *Shaffer v. Regions Fin. Corp.*, 29 So. 3d 872, 880 (Ala. 2009). These requirements apply to implied contracts as well as express contracts. *Ellis v. City of Birmingham*, 576 So. 2d 156, 157 (Ala. 1991) ("A contract implied in fact requires the same elements as an express contract . . . ."). The only difference between a breach of contract and a breach of implied contract is how the contract was formed. "Implied contracts normally arise in situations where there is a bargained-for exchange contemplated by the parties, but no overt expression of agreement." *Id.*

Warrior contends that Mr. Gibson does not state a claim for breach of an implied contract because (1) he suffered no damages and (2) he does not allege that he and Warrior mutually agreed to the security procedures Warrior would use. (Doc. 12-1 at 38–39). The court rejects the first argument because, as already discussed, Mr. Gibson has adequately alleged damages.

With respect to mutual assent, Mr. Gibson alleges that Warrior required disclosure of personal identifying information as a condition of employment and it promised him that it would keep his data safe, confidential, and private. (Doc. 1 ¶¶ 27–28, 54, 140). Warrior contends this is insufficient to establish mutual assent because no allegations indicate that it believed or expected it would provide the security procedures Mr. Gibson expected. (Doc. 12-1 at 38). But Mr. Gibson alleges that Warrior's website stated it had "implemented measures designed to secure your Personal Information from accidental loss and from unauthorized access, use, alteration and disclosure" (doc. 1 ¶ 28), and that Warrior's written privacy policies promised "only [to] disclose Private Information under certain circumstances, none of which relate to the Data Breach" (*id.* ¶ 215). And contrary to the argument Warrior raises in its reply brief, Mr. Gibson's citation to the privacy policy presents a sufficient basis to reasonably infer Mr. Gibson read it. (*See id.*); *Gates*, 884 F.3d at 1296.

The court declines to address Warrior's argument that, to the extent the parties agreed that Warrior would provide "reasonable security," Warrior fulfilled its obligation, because Warrior did not raise that argument in its initial brief. (*Compare* doc. 21 at 13, *with* doc. 12-1 at 38–39); *see Herring v. Sec'y, Dep't of Corr.*, 397 F.3d 1338, 1342 (11th Cir. 2005) ("[A]rguments raised for the first time in a reply

brief are not properly before a reviewing court."). The court **WILL DENY** the motion to dismiss Count Three.

d. Count Four: Invasion of Privacy

Mr. Gibson alleges that Warrior is liable for wrongful-intrusion invasion of privacy because it permitted the data breach knowing its security practices were inadequate. (Doc. 1 ¶¶ 230–31).

The tort of invasion of privacy is the "intentional wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities." *Reg'l Prime Telev. v. South*, __ So. 3d __, 2024 WL 997698, at *12 (Ala. March 8, 2024). (quotation marks omitted). There are four types of invasion of privacy, *see id.*, and Mr. Gibson's claim is limited to the wrongful-intrusion type. (Doc. 1 ¶ 230). Under that type of invasion of privacy, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Reg'l Prime Telev.*, 2024 WL 997698, at *13 (quotation marks omitted).

Warrior argues Mr. Gibson fails to state a claim for invasion of privacy because the tort requires *Warrior* to intentionally intrude Mr. Gibson's solitude or seclusion. (*See* doc. 12-1 at 40–41). It argues that, even if its cybersecurity was

inadequate, passively allowing someone else to intrude on Mr. Gibson's privacy cannot establish liability against Warrior. (*Id.*). Mr. Gibson responds that under Kentucky law, a defendant's reckless disregard for a plaintiff's privacy can suffice to show intentional conduct for purposes of wrongful-intrusion invasion of privacy. (Doc. 16 at 40–41). He argues that because Kentucky and Alabama both follow the Restatement (Second) of Torts, Alabama also permits reckless conduct to satisfy the intentionality requirement. (*Id.* at 41).

Nothing in the Alabama caselaw indicates that Alabama courts would find a defendant's reckless conduct sufficient to show that the defendant "intentional[ly] wrongful[ly] intru[ded] into one's private activities." *Reg'l Prime Telev. v. South*, 2024 WL 997698, at *12; *see also* Restatement (Second) of Torts § 652B comment. (c) (2024) ("The *defendant* is subject to liability . . . only when *he* has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs.") (emphasis added). The complaint contains no allegation that Warrior intentionally intruded on Mr. Gibson's solitude or seclusion, nor does Mr. Gibson otherwise respond to Warrior's argument that the complaint lacks those allegations. (*See id.*). Accordingly, the court **WILL GRANT** the motion to dismiss Count Four.

e. Count Five: Unjust Enrichment

Mr. Gibson alleges that Warrior is liable for unjust enrichment because he conferred a benefit on Warrior by providing it with his labor, Warrior accepted the benefit, and Warrior enriched itself by using cheaper, ineffective security measures. (Doc. 1 ¶¶ 240–43). "To prevail on a claim of unjust enrichment under Alabama law, a plaintiff must show that: (1) the defendant knowingly accepted and retained a benefit, (2) provided by another, (3) who has a reasonable expectation of compensation." *Matador Holdings, Inc. v. HoPo Realty Invs., LLC*, 77 So. 3d 139, 145 (Ala. 2011).

Warrior contends that Mr. Gibson has not alleged that it accepted and retained a benefit it did not pay for because it paid Mr. Gibson for his labor and he has not provided specific allegations about the cost or effectiveness of its security measures. (Doc. 12-1 at 42–43; *see also id.* at 22–23). But Mr. Gibson alleges that disclosure of his personal identifying information was a condition of employment (doc. 1 ¶¶140), that Warrior promised to keep the information secure (*id.* ¶¶ 27–28, 54), and that he would not have given the information to Warrior if he had known Warrior would not protect it (*id.* ¶¶ 18, 141, 246). It is reasonable to infer from these allegations that Mr. Gibson would not have accepted employment with Warrior if he believed that Warrior was not going to adequately protect the information, so that Warrior's protection of the data was a benefit of employment. *See Gates*, 884 F.3d

at 1296. Moreover, Mr. Gibson alleged a variety of specific security precautions that Warrior should have taken but did not take, to its financial benefit. (Doc. 1 ¶¶ 41, 43–46, 243). At this stage, the allegations are sufficient to make out a claim that Warrior received the benefit of Mr. Gibson's labor in exchange, in part, for a promise to protect Mr. Gibson's data, but Warrior saved money by using less costly and less effective security measures. Accordingly, the court **WILL DENY** Warrior's motion to dismiss Count Five.

f. Deficiencies in Warrior's Notice

In the factual allegations section of his complaint, Mr. Gibson alleges that the notice Warrior sent to affected individuals after the breach was deficient for several reasons, including its untimeliness, its failure to explain the cause of breach, and its failure to describe Warrior's remedial measures. (Doc. 1 ¶¶ 35–37). In its motion to dismiss, Warrior disputes those allegations but makes no argument about how the adequacy of the notice affects the claims against it. (Doc. 12-1 at 43). So the court does not consider Warrior's disputes with Mr. Gibson's allegations regarding the adequacy of the notice.

III. CONCLUSION

The court **WILL GRANT IN PART** and **DENY IN PART** Warrior's motion to dismiss. (Doc. 12). The court **WILL GRANT** the motion to dismiss all of Mr. Gibson's requests for injunctive except the request to educate class members

about the threats they face and steps they must take to protect themselves **WITHOUT PREJUDICE** for lack of standing. The court **WILL GRANT** the motion to dismiss Count Four for failure to state a claim. The court **WILL DENY** the motion to dismiss Counts One, Two, Three, and Five.

The court will enter a separate order consistent with this opinion.

DONE and **ORDERED** this October 3, 2024.

ANNEMARIE CARNEY AXON
UNITED STATES DISTRICT JUDGE